IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

DECLARATION OF DAVID CROSS
IN SUPPORT OF MOTION FOR DISCOVERY

DAVID D. CROSS, declares, under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. My name is David D. Cross and I am counsel for Plaintiffs in this matter. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. My firm, Morrison & Foerster, has extensive experience reviewing, handling, and storing highly sensitive and confidential material. Our work regularly requires us to maintain documents and information under secure conditions approved by financial regulators, financial institutions, Fortune 500 companies, and foreign governments. In many cases, such as those involving

financial confidential supervisory information, civil and/or criminal penalties apply to the dissemination of such materials. And in other cases, we are required to review information, including source code information, reflecting trade secrets. As such, I am confident that we can maintain any GEMS-related information or data under conditions of the utmost security.

3. John P. Carlin, former Assistant Attorney General for the U.S. Department of Justice's National Security Division, currently serves as co-chair of Morrison & Foerster's National Security practice group. Until 2016, Mr. Carlin served as the DOJ's highest-ranking national security attorney, and, in that capacity, oversaw nearly 400 employees responsible for protecting the nation against terrorism, espionage, and cyber and other national security threats.

4. Mr. Carlin will assist our team in developing and implementing any protocols used to ensure the security of any information related to the GEMS database. Mr. Carlin's professional biography is attached as Exhibit A to this Declaration.

5. In response to the Court's July 2, 2019 Order regarding Plaintiffs' discovery requests related to the State's GEMS database and server, and the terms of a proposed protective order, Morrison & Foerster, as counsel for Plaintiffs, is prepared to implement the security protocols outlined below.

6. Plaintiffs propose installing copies of the GEMS database onto a limited number of air-gapped, password-protected, standalone computers that are not connected to the internet (the "Protected PCs"). The number of Protected PCs would be specified by the Court.

7. In my experience, multiple computers would be necessary given the fact that Plaintiffs' attorneys and designated experts would likely need to work in parallel. This is particularly so, given the expedited nature of this litigation.

8. The Protected PCs would be kept at all times in locked, secure work areas, to which only Plaintiffs' attorneys and designated experts had access. Such areas would be subject to twenty-four hour video surveillance. The Protected PCs would be password protected. Under no circumstance, would the Protected PCs be permitted to leave the secure work areas. Additionally a log of all access to the secure work areas and to the Protected PCs would be maintained.

9. To avoid any confusion, the Protected PCs would be clearly identified and labeled as such.

10. Plaintiffs' attorneys and designated experts would be permitted to bring their own laptops into the secure work areas. Beyond material required to analyze the GEMS database, no additional equipment or materials would be permitted in the secure work areas.

11. Under no circumstances, would the GEMS database be installed on any non-Protected PC or device. While attorneys and designated experts would be permitted to use external hard disks and removable storage media (e.g., USB dongles, CD-Rs, DVD-Rs) on their own laptops or other devices, such devices would never be permitted to be installed or introduced into a Protected PC.

12. In addition to the above-outlined protocols, we are prepared to implement any additional restrictions that the Court may require.

13. In my experience, the above-outlined protocols will be more than sufficient to ensure the security of any GEMs-related information or data. Moreover, my firm has the experience and capability to ensure that these protocols are effectively implemented and enforced.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 3rd day of July, 2019 in San Francisco, California.

/s/ David D. Cross
David D. Cross

EXHIBIT A

MORRISON FOERSTER

John P. Carlin

PARTNER

2000 PENNSYLVANIA AVENUE, NW
SUITE 6000
WASHINGTON, D.C.
20006-1888
(202) 463-1000
250 WEST 55TH STREET
NEW YORK, NY 10019-9601
(212) 336-8600
JCARLIN@MOFO.COM

EDUCATION

WILLIAMS COLLEGE (B.A., 1995)
HARVARD LAW SCHOOL (J.D., 1999)

BAR ADMISSIONS

NEW YORK
DISTRICT OF COLUMBIA

PRACTICES

GLOBAL RISK + CRISIS MANAGEMENT
NATIONAL SECURITY, CFIUS, SANCTIONS + EXPORT CONTROLS

John P. Carlin, former Assistant Attorney General for the U.S. Department of Justice's (DOJ) National Security Division (NSD) and former Chief of Staff to then-FBI Director Robert S. Mueller, III, chairs Morrison & Foerster's Global Risk and Crisis Management practice group and is co-chair of the National Security practice group. Mr. Carlin, who served as a top-level official in both Republican and Democratic administrations prior to joining Morrison & Foerster, regularly advises industry-leading organizations in sensitive cyber and other national security matters, internal investigations, and government enforcement actions.

Mr. Carlin is routinely called upon to advise leading U.S. and overseas companies across numerous industries—including in the technology, healthcare, energy, defense, finance, fashion, media, pharmaceutical, and telecommunications sectors—regarding crisis management, cyber incident response and preparedness, regulatory strategy, and CFIUS. Clients appreciate that Mr. Carlin, who served until 2016 as the DOJ's highest-ranking national security lawyer, can offer an insider perspective on their matters and is able to quickly engage the appropriate government actors in the event of a cyberattack or other significant incident affecting their business.

Selected Significant Representations

- **Advised on breach incidents.** Advised global companies, including Fortune 50, in response to cyber incidents.
- **Cybersecurity training.** Advised international consulting companies on their privacy and data security issues and provides onsite training exercises to board and executive members.
- **Breach and ransomware response.** Advised companies on ransomware policy, as well as response to incidents.
- **CFIUS strategy.** Advised major foreign investment companies on both their near-term and long-term CFIUS strategy, including about the implications of recently enacted reform legislation that will significantly affect the way CFIUS reviews are conducted.
- **Compliance and risk assessment.** Conducted compliance and risk assessments as well as advised on cybersecurity incidents and legislative issues to global technology firms.
- **Sanctions and Trade.** Consulted on the impact of U.S. sanctions policy to major international corporations.
- **Export Controls.** Conducted investigations and advised on compliance policies and procedures.
- **Crisis incident simulation.** Provided various crisis incident simulations as well as table-top exercises to members of executive teams to international companies.

In his previous role as Assistant Attorney General for National Security, for which Mr. Carlin was nominated by the President and overwhelmingly confirmed by the Senate on a bipartisan basis, he oversaw nearly 400 employees responsible for protecting

the nation against terrorism, espionage, and cyber and other national security threats. Under his leadership, the NSD:

- Created a threat analysis team to study potential national security challenges posed by the Internet of Things;
- Launched a nationwide outreach effort across industries to raise awareness of national security, cyber, and espionage threats against American companies and encourage greater C-suite involvement in corporate cyber security matters;
- Oversaw DOJ's Counterintelligence and Export Control Section, responsible for investigating and prosecuting espionage cases, cases involving the illegal export of military and strategic commodities, and cases involving certain cyber-related activity;
- Brought an unprecedented indictment against five members of the Chinese military for economic espionage;
- Investigated the attack on Sony Entertainment's computer systems;
- Brought charges, in conjunction with the FBI, against seven Iranians working for Islamic Revolutionary Guard Corps-affiliated entities for conducting a coordinated campaign of cyber attacks against the U.S. financial sector;
- Prosecuted major sanctions and export controls matters, including significant civil and criminal penalties against major global actors and noteworthy cases against malicious cyber actors;
- Oversaw the efforts of the National Security Cyber Specialist Network and the National Security/Anti-Terrorism Advisory Council program;
- Led DOJ's participation on the Committee on Foreign Investments in the United States;
- Disrupted multiple terrorist plots and national security threats, bringing those involved to justice; and
- Prosecuted the Boston Marathon bombing case; and
- Provided legal oversight of the NSA's surveillance activities and represented the government before the Foreign Intelligence Surveillance Court.

Prior to assuming his role in the NSD, Mr. Carlin served as Chief of Staff and Senior Counsel to Robert S. Mueller, III, former director of the FBI, where he helped lead the FBI's evolution to meet growing and changing national security threats, including cyber threats. Mr. Carlin also held positions as National Coordinator of DOJ's Computer Hacking and Intellectual Property Program and Assistant United States Attorney for the District of Columbia, where he prosecuted cyber, fraud, and public corruption matters, among others, trying more than 40 cases to verdict.

Mr. Carlin is an inaugural Fellow of the Harvard Kennedy School's Belfer Center for Science and International Affairs' Homeland Security Project, focused on the unique challenges and choices around protecting the American homeland. He also chairs the Aspen Institute's Cybersecurity and Technology policy program, which provides

a cross-disciplinary forum for industry, government, and media to address the rapidly developing landscape of digital threats and craft appropriate policy solutions.

Mr. Carlin, who joined DOJ through the Attorney General's Honors Program, is a five-time recipient of the Department of Justice Award for Special Achievement, was awarded the National Intelligence Superior Public Service medal by the Director of National Intelligence, and has drawn bipartisan praise, with U.S. Attorney General Loretta Lynch calling him "a trusted and tireless leader" and former U.S. Attorney General Michael Mukasey calling him "a superb civil servant." He earned his Juris Doctorate from Harvard Law School, where he received the Samuel J. Heyman Fellowship for Federal Government Service and served as Articles editor for the *Harvard Journal on Legislation*, and earned his Bachelor of Arts degree, *magna cum laude*, from Williams College, where he was elected to Phi Beta Kappa.